XporY Control-Plane (CP) — Documento Técnico

> **Escopo:** Governança, políticas, credenciais (PKI/JWT), auditoria, telemetria e cálculo/gestão de desbalanço. Este doc foca no **como**.

---

1. Objetivos

- Centralizar políticas (importação, visibilidade, export delay, FX, limites) e distribuir com baixa latência.
- Ser autoridade de identidade (mTLS/JWT) e de risco (desbalanço → signals).
- Coletar telemetria/ledger para BI e auditoria.

2. Não-Objetivos

- Não participar do caminho crítico do checkout (apenas observador/sinalizador).

3. Arquitetura Lógica

- **API Policies** (read-mostly)
- **Service PKI/JWT** (emissão/rotação)
- **Risk Engine** (desbalanço + signals)
- **Telemetry Ingest** (append-only)
- **Admin UI** (governança)

4. Decisões (ADR Snapshot)

- CP fora do data-plane; cache TTL 1–5min nos WLs.
- PKI corporativa + JWT curta duração (≤5min), *least-privilege scopes*.

- Signals assíncronos com confirmação de recebimento pelos WLs.

5. Contratos — Descrição dos Endpoints

- **GET /wls**, **POST /wls** — cadastro/consulta de WLs.
- **GET/PUT /wls/{id}/policies** — pacote de políticas do WL.
- **GET/PUT /relationships/{src}/{dst}** — FX/limite/status entre pares.
- **POST /policies/pull** — endpoint para Policy Agent.
- **POST /imbalance/signals** — emissão de bloqueio/desbloqueio.
- **POST /telemetry/events** — ingestão de eventos/ledger.
- **GET /reports/trade-balance** — série consolidada.

6. Modelo de Dados (resumo)

- `cp_whitelabel`, `cp_policies`, `cp_relationships`, `cp_imbalance_signals`, `cp_telemetry`.

7. Segurança

- mTLS obrigatório; CA XporY; rotação a cada 90 dias (automatizada).
- JWT assinado pelo CP; JWKs públicos; *token binding* por WL.
- Rate limiting por cliente/WL e *WAF* para CP.

8. Observabilidade

- Tracing distribuído (OpenTelemetry)
- Métricas: latência de pull, *policy drift*, throughput de signals.
- Logs com *correlation-id* e *redaction* de PII.

9. SLOs

- Disponibilidade 99,9%; p95 `GET policies` < 150ms; *policy drift* ≤ 5min.

10. Migrations (Liquibase Groovy — extratos)

- Incluiremos os blocos groovy no anexo técnico.

11. Testes

- Contract tests (CP↔WL), validação de FX/limites por par, idempotência de signals.

12. Playbooks

- Rotação de certificados, *keys rollover*, degradação do Risk Engine, atraso de ingest.

13. Rollout

- Piloto com 2 WLs; *feature flags* de escopo; *canary* para Risk Engine.